Proposed Smart Card Interoperability Framework for FIPS 201

NIST
October 18, 2004

1. Overview

The Government Smart Card(GSC) community has been moving toward formal smart card interoperability standards since the inception of the GSC program. The most recent version of the GSC Interoperability Specification was published in 2003 as NIST Interagency Report 6887 (also known as GSC-ISv2.1). GSC-ISv2.1 is not a formal standard, but serves as the basis for the U.S.-led effort to develop an ISO suite of standards for smart card interoperability. This ISO standards suite is known as ISO 24727.

GSC-ISv2.1 supports two "virtual" card interfaces that must be mapped to native card interfaces in middleware via the Card Capability Container stored on each card. In other words GSC-ISv2.1 does not define a hard card platform, but abstracts the differences between cards in middleware. This imposes significant complexity on GSC-ISv2.1 middleware and makes standardized card management difficult. In other words, GSC-ISv2.1 is based on a lightweight card model and a heavy middleware model.

Homeland Security Presidential Directive 12 instructs NIST to produce a Federal Information Processing Standard for Personal Identity Verification(PIV) by February, 2004. Among other things, the PIV (FIPS 201) requires a standardized, interoperable smart card platform and a core set of credential elements. The PIV card platform will be based on GSC concepts, but must also consider the ongoing formal standards work within ISO. NIST believes that HSPD-12 should be taken as an opportunity to move the GSC community toward the ISO standards suite. The GSC framework has already moved beyond GSC-ISv2.1 through the addition of the PACS and FICC Data Model specifications. Although there is a cost to this migration, the long term cost will be greater if the government continues to field GSC-ISv2.1 compliant systems over the next several years. GSC-ISv2.1 was a significant step forward, but it has not solved all of the interoperability problems that need to be addressed for a true governmentwide rollout of smart card technology.

NIST has proposed a significant evolution of the Government Smart Card interoperability framework for FIPS 201. This evolution eliminates the need for a Card Capability Container, and has the following advantages over the existing GSC-ISv2.1:

- Reduces middleware complexity

- Facilitates development of a unified card management model and infrastructure

- Aligns with PACS and the FICC data model framework

- Provides a clear migration path to ISO 24727

This document provides an overview of the proposed PIV smart card interoperability framework. The full technical specification of this architecture can be found in FIPS 201(Draft), October 19 2004.

2. Card Platform

The PIV card platform consists of a card manager application and a cryptographic information application. The card manager application is present on all PIV cards, and presents a standard, ISO compliant set of card platform commands that support card management, cardholder authentication, and generic file management. Because the PIV card platform defines a "hard" card interface, there is no need for the GSC-ISv2.1 CCC-based mapping mechanisms. The PIV card interface can be extended by adding card applications that support additional card application commands.

The cryptographic information application is an on-card database of information about the cryptographic capabilities and credential elements of the card. This application is a compliant subset of ISO/IEC 7816-15. The proposed PIV card platform therefore replaces the GSC-ISv2.1 proprietary Card Capability Container mechanisms for managing cryptographic and credential elements with a standards compliant approach.

The core PIV card platform commands are summarized below:

Type	Name	Secure Messaging	Command Chaining
Card Commands for Card Content Management	**CARD CONTENT MANAGEMENT REQUEST**	Yes	No
	LOAD	No	No
	DELETE APPLICATION	No	No
Card Platform Commands for Application Management	**GENERATE ASYMMETRIC KEY PAIR**	Yes	Yes
	SELECT APPLICATION	No	No
Card Platform Commands for Data Management	**CREATE FILE**	Yes	Yes
	DELETE FILE	No	No

Management	**SELECT FILE**	Yes	No
	GET DATA	Yes	No
	PUT DATA	Yes	Yes
	SEARCH BINARY	Yes	No
	READ BINARY	Yes	No
	UPDATE BINARY	Yes	Yes
Card Platform Commands for Authentication	**EXTERNAL AUTHENTICATE**	Yes	Yes
	GET CHALLENGE	No	No
	INTERNAL AUTHENTICATE	Yes	Yes
	VERIFY	Yes	No
	CHANGE REFERENCE DATA	Yes	No
	RESET RETRY COUNTER	Yes	No
	MANAGE SECURITY ENVIRONMENT	Yes	No
	PERFORM SECURITY OPERATION	Yes	Yes

3. Data Structures

PIV supports both file-based and object-based card architectures through the concept of data elements. A data element is an item of information seen at the card command interface for which a name, description of logical content, a format, and a coding are specified. A data element is either a transparent file identified by a two-byte File ID (FID) or a data object identified by a BER-TLV Data Object Tag (DOT). A transparent file may contain data objects, in which case it is called a BER-TLV file. A constructed data object is a data object that contains other data objects.

Each PIV card contains one or more file systems, each having a unique AID. The root of a file system, identified by an AID, is an application dedicated file (ADF). A PIV card may contain a distinguished root called the master file (MF). Each data element is therefore uniquely identified by an AID followed by a sequence of zero or more FIDs, BER-TLV FIDs, or DOTs, and terminated by an FID or DOT.

Data types supported by the PIV card:

Access Control Rule

Algorithm Identifier

Application Identifier

Application Properties

Authenticator

Connection Description

Data Object

Data Element Name

Data Element Properties

Handle

Reference Data Identifier

Length

Offset

Secure Channel Type

Status Word

4. Security Architecture

An access control rule is associated with every card application, every dedicated file, every transparent file, and every data object on the PIV card. Access control rules define the relationship between principals, data elements, and operations that can be performed on data elements. Each principal is uniquely identified by a reference data identifier that points to the information used to authenticate that principal (PIN, password, etc.). Each principal has an associated security status indicator that is TRUE if that principal's credentials have been authenticated by the card and FALSE otherwise.

A selected application's current security environment consists of a set of data objects that parameterize the cryptographic operations that can be performed by the application. The MANAGE SECURITY ENVIRONMENT command creates and changes data objects in an application's current security environment.

Each PIV card contains a cryptographic information application in accordance with ISO 7816-15. The AID of the cryptograpic information application is 'E8 28 BD 08 0F 00'. The dedicated file associated with this AID is DF.CIA. Cryptographic information files managed by the cryptographic information application include:

EF.CardInfo: FID '5032', version number of CIA

EF.OD: FID '5031', paths to private keys, public keys, secret keys, certs, authentication objects

EF.PrKD: Private key description file

EF.PuKD: Public key description file

EF.SKD Secret key description file

EF.CD: Certificate description file

EF.AOD Authentication object description file

Secure messaging and command chaining are supported.

5. Client API

The PIV draft specifies a client application programming interface equivalent to the Basic Services Interface in GSC-ISv2.1. The primary differences between the two are the addition of card management entry points and modifications to explicitly support secure channel establishment and data element management. The PIV client application programming interface is summarized below:

Entry Points for Communication	**Connect**
	Acquire Context
	Establish Secure Channel
	Release Context
	Disconnect
Entry Points for Card Application Management	**Add Card Application**
	Delete Card Application
	Generate Key Pair
	Import Key
	Get Card Application Properties
Entry Points for Data Management	**Create Data Element**
	Delete Data Element
	Select Data Element
	Get Data Element Properties
	Read Data

	Write Data
Entry Points for Authentication	**Authenticate Card**
	Authenticate Principal
	Get Certificate
	Get Challenge
	Create Digital Signature
	Verify Digital Signature

6. Card Management

Operations on a PIV card that create, alter or delete critical security parameters or create or delete data structures are generally referred to as card management operations. Examples of card management operations include the generation of a private key on the card or the creation of a new data file on the card

Typically card management operations are only performed by the card issue or an application provider although a cardholder changing their PIN is strictly speaking also an example of a card management operation. Card management includes both card personalization – making the card ready for use by a particular individual – and card administration – adding a application to the card.

Card management operations are differentiated from card use operations because they utilize commands, communication protocols and cryptographic algorithms that are not used during normal card usage. The ISO standard ISO/IEC 7816-9, entitled "Interindustry commands for card and file management" describes the ISO commands and procedures that are used for card management whereas the ISO standard ISO/IEC 7816-4, "Organization, security and commands for interchange" describes the ISO commands and procedures that are used in everyday use.

The FIPS 201 Card Manager is a card application that is present on every FIPS 201 card and it is the on-card representative of the card issuer. A card management client-application is a client-application that interacts exclusively with the Card Manager. The Card Manager in turn interacts with the various application domains on the card to perform card management operations.

In interacting with the Card Manager, a card management client-application may use many of the same FIPS 201 client-application application programming interface entry points that a non-managment card application uses. A card management application, for example, has to establish communication with the card and often has to read and update existing files on the card.

These client-application programming interface entry points generate card-edge

commands that are exactly the same card-edge commands generated by non-management applications with one important difference. Card management client-applications use a secure channel to communicate with the Card Manager.

The beginning of a card management session from the point of view of calls the card management client-application places on the FIPS 201 Client-Application Programming Interface looks like this:

1. Establish communication with the card
   ```
   Connect
   Acquire Context
   ```

2. Select the Card Manager application
   ```
   Select Card Application
   ```

3. Establish a secure communication channel with the Card Manager
   ```
   Establish Secure Channel
   ```

The Card Manager application (on behalf of the card issuer) is charged with insuring that a recognized principal is performing card management operations and furthermore that this recognized prinicipal is authorized to perform the card management functions being requested.

The Card Manager application accomplishes this by analyzing the cryptography applied to card management requests. Simply put, if the keys applied to a request are associated with a principal that is authorized to perform the request, then the request is granted. Otherwise, the request is rejected.

7. Summary

The proposed PIV smart card interoperability framework represents a major step forward for the GSC community. Although there are costs associated with this migration, the overall cost to the government will be greater if FIPS 201 mandates large scale deployment of GSC-ISv2.1 systems. The final objective is to move toward the long term stability that will be provided by formal ISO standards. The gap between GSC-ISv2.1 and ISO 24727 is far greater than the gap between the proposed PIV framework and ISO.